EX PARTE OR LATE FILED

Steve Cichosz
3551 Keystone Loop
Discovery Bay CA, 94505
925-344-4311
Steve@TekAdvocates.com
December 22, 2011

10-90

Subject: Internet end user privacy

Chairman Genachowski
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Dear Chairman,

The Internet today has transcended to becoming an entirely different operating environment than the rules under which it currently functions can be expected to credibly support. Since being opened to commercial operation in 1995 subtle incremental changes have taken place shifting from a level playing field as an information source for end users, to becoming an environment advantageous to commercial entities through information extraction *from* end users. This fact in combination with the naiveté of the general population on the implications of their internet activities creates an unfair marketplace unbeknownst to the increasingly disadvantaged end user.

The early approach of self-regulation, as explained in the Safe Harbor act, was a considerably more effective model when end user data interaction was with single entities having a vested interest in keeping their collected data secure. As an example; when a merchant collected end user data, whether online or loyalty program strategies were utilized, costs were associated with gathering this information. These costs were expected to be recouped directly back from the end user through enhanced services and marketing strategies ultimately manifesting as a competitive advantage for the merchant. The merchant had a vested interest in treating the collected information with reverence to both prevent customer discontent and maintain their competitive advantage over other merchants. This interaction was in effect a one-on-one conversation between customer and merchant with an understanding of the information collected, where it would be maintained, how it would be used and how it would be protected.

In today's online marketplace information is becoming increasingly centralized creating opportunities for activities deeply intrusive and blatantly abusive to end user privacy. Companies are rising, especially in the social network space, that have business models built upon the harvesting and reselling of the data once kept in confidence. Where end user data collection was once undertaken almost exclusively as an ancillary activity in support of a company's core business, businesses are now being built upon the practice of selling the user data itself. In this

paradigm shift an approach of self regulation to assure data protections cannot work. The deeper the need realized by a company harboring unprotected user information, the greater the data intrusive activities will become.

The holy grail of any marketing company is to achieve an emotional response from their target market. In many cases there is indifference as to whether that be a positive or negative response, only that the target of their efforts be reached emotionally. In mining the often deeply intimate data provided by the end user as User Generated Data (UGD) in the form of conversational activity on the Internet, the marketer is able to gain deep insight into the very psyche of those analyzed. Education level, financial position and even health assessments can be drawn from the uninhibited conversations taking place on the Internet. Existing regulations such as the Financial Data Protections Act of 2006 and HIPAA are being rendered irrelevant through analysis of UGD. Simple analysis of hosted emails passed between, friends, relatives and in which commerce is conducted; will reveal any information currently protected by privacy legislation of all forms. User generated conversations in social media can be, and are, analyzed to secure sophisticated profiles for the end users generating this data. While currently known profiles are advertised as being de-identified cross segments of the population, such profiling activities are exercises in social opportunity containment and in their very nature are having an absolute minimum impact of acting as screens for the information presented to the subjects of the profiling.

Some of the deeper impacts of these data abuses manifest as the increased effectiveness of manipulative marketing practices, information propagation uncertainties, guilt by association isolationism and influence theft.

Increased manipulation effectiveness

Marketing in its pure sense is an age old and necessary practice of making prospective customers aware of a product to be offered. Market analysis to effectively identify potential customers that would most benefit by a product is a reasonable aspect of this marketing. Marketing crosses an ethical boundary when it becomes an exercise in persuasion and becomes outright immoral as an exercise in manipulation. The act of market analysis to determine, not who would most benefit by a product, but rather how to best manipulate the populace into buying a product, whether it would benefit them or not, is bad business. The deep personal analysis now possible with the prevalence of UGD creates an unprecedented ability to manipulate the populace into buying products based on subliminal emotional responses rather than on the merits of the product or service itself.

Information propagation uncertainties

In past interactions involving data collection, a customer could conduct business with a reasonable level of confidence as to the information that was known about them by the institution they were engaging. These assurances were justified in the knowledge that information relevant to the transaction would not be repeated outside the institution with which the interaction took place. Vehicles for communicating customer details, such as credit reporting institutions, remain highly regulated with rigid rules around the transparency of the information communicated and who may access this information. In the contrast of todays paradigm of managing UGD, the end user has no way of knowing how they have been profiled, nor is there any way of knowing who is using the information profiles into which they have been categorized. This is a serious disadvantage for a potential customer to not only be naive as to what is known about them, but also who knows it.

Guilt by association

A deep understanding and analysis need not be accomplished on every end user populating a UGD storing database for customer disadvantages to be realized. The concept of "guilt by association" is the key result of analysis simply conducted on the premise of who an end user knows, the "friends" and "friends of friends" concepts. The established theory is that end users are fundamentally like those which whom they associate. As one important example of this activity "Yahoo News" reported by way of a "Mashable.com" October 7, 2011 article titled "What Banks and Lenders Know About You from Social Media" that banks are beginning to use the financial stability of an end users associates as a consideration in lending to them. This means that simply being associated with a profiled social circle, as unwittingly defined by one's online interactions, could negatively impact one's ability to conduct commerce, or one's life in general, with no understanding for why these impacts are taking place.

Influence theft

Purveyors of the centralized social network are continuously analyzing the influence of the end users utilizing their offerings. Once a practice exclusive to celebrities with an understanding for how to capitalize on the value of their influence, the common end user is now closely scrutinized for the same. This measurement of influence within the social network is calculated and considered in the advertising strategies of companies conducting analysis on the personal, UGD of unwitting end users. Where celebrities are paid for their heightened influence the average end user is manipulated into being product spokesman of a "heightened value" without their knowledge or compensation for participating in a targeted advertising campaign.

At the center of the principles upon which our nation was built into being the mightiest society on the planet is that of the individual citizen being free to live their life without undo, undesired influence by a governing body through intrusive behavior. So important are these principles that every state of the union has ruled that the Miranda Rights are read to alleged criminals in order to ensure they are aware of their privilege to remain silent, that a few misplaced words of explanation would not be used against them. Today every intimacy of the approximately 63% of Americans using the social network is accessed and analyzed in sophisticated ways they could not reasonably be expected to understand and in turn used against them in the marketplace.

While solutions are certain to meet unflinching opposition from those who benefit from the imbalance of today's current data invasive practices, solutions not overly complicated to implement are not far off. Of the many avenues to approaching these issues, six stand out as having the greatest impact towards leveling the marketplace without imposing unprecedented and unreasonable constraints upon honorable businesses.

Intent of use law

User generated data must not be used for any purpose other than intended by the end user as would be reasonably expected under the auspices of services advertised to that end user. Any form of data provided by the end user is to be treated as personal property and made accessible only to the computers of the originators intended audience and restricted only to the computers of the service provider required to provide the subscribed service. Business partners of the service provider should be permitted access only to end user data necessary to perform the subcontracted functions and rarely have access to UGD.

Collecting domain regulation

Services and merchants collecting user generated data must ensure collected data remain accessible only from the domain under which it was collected except when the collecting agent has a customer relationship in acquiring third party support necessary to providing the requested service to the end user. Any third party relationship requiring release of UGD is to be concisely documented to include the data recipient, purpose of transmission and the data transmitted.

Profiling

Analysis/profiling of end user actions as required to improve offerings specific to the service domain is a necessary and permissible activity. Examples of reputable analysis would be those of site visits, page views and purchase history. Any form of analysis or profiling in regard to end user psyche, personality, health, and physical characteristics must not be permitted. Demographic information such as gender, race, age, region of residence or income based on data expressly provided by the end user is permissible, programmatic analytical derivation of demographic data not expressly provided by an end user is not to be permitted.

Email regulations

Email is to be managed under the same protections afforded the United States Postal Service. In the current age of electronic commerce, financial, health and deeply intimate personal conversations take place in the virtual mail space as abundantly as the physical mailing realm. The electronic mails of our current society are no less imperative to the individual or any other business entity than the communications transpiring in the physical mail managed by the USPS. Email communication should be no less subject to protections against in transit reading or other tampering by humans or machines than the current physical medium.

Redefine "identifying data"

IP address and any other information enabling return communication in any medium must be considered "identifying data." If an end user may be contacted by means of a specific datum, then by definition that datum is identifying information as an individual must first be identified before effectively being the recipient of a communication.

Implied sensitivity

User generated data for which security protections to inhibit access by others [redacted] of a service are offered is to be treated as with the reverence of customer sensitive data. The service provider, except as necessary to provide the specifically subscribed services, shall operate under the same access restrictions as implied by the end users strictest public interface privacy settings.

FCC proceedings 09-51 and 10-90 are important objectives and essential to assuring all Americans rise with the current technological tide. However to undertake such endeavors without adequate end user protections is a greater service to marketplace predators than to the citizenry being exposed to them.

While over regulation is a stifling practice that impedes the innovation and prosperity of creative companies seeking to stretch beyond the current norms, there are times well considered regulation must be imposed to prevent such ventures from straying into directions counterproductive to the best interests of our citizenry. The

current privacy invasive activities of the centralized social repositories are creating a seriously inappropriate imbalance in the competitive framework of the nations broadband interactions. Common end user sentiment is that of discontent and frustration over having no choice but to suffer the abuses prevalent and beyond their control on what has now become a vital communications framework. It is important these recommended regulatory policies, rooted more in best practice than profit enhancement, with the objective of assuring the integrity of our nations quickly evolving communication technologies, be implemented promptly. Failing to assure the integrity of our citizenries privacy by curtailing the infractions of today will foster an unmanageable data environment rich in opportunities for intrusive privacy atrocities as our destiny.

Respectfully,

Steve Cichosz

cc: Commissioner Clyburn,
Commissioner Copps,
Commissioner McDowell
Congressman McNerny